

## Theory of Data-Limited Information

This theory proposes the generalized concept that any data that is available into reality is limited. There are stages that this theory proposes but before that, there is a type of Data dispersion. The first one is the data dispersion through amount boundary. This type refers to the ones that we have limited access depending on how much data or power was given to us by a source. Data and power are the terms used to explain information from the net, any value equivalents that express message or value, anything that works to input and output. Input and output are the ones in the system e.g. a program where a series of code may change the input directly or the process of a transaction between input and output. By source, it's the data that the telecommunication companies control to distribute different values into different users. A company or any data distributor that has the authority to manipulate the given amount of data depending on the contract between a client and a source. The data that will be given and will be used and end at a specific length of usage. The second type of data dispersion is deletion. It could come in two ways on how it will be executed. First is when a person that has the right to the data's amount could delete the amount of data on his own will. The second is when the source deletes it without any indicators beforehand e.g. source deleting a data from the server that affects the users. The third is the outside interference which comes from intervention of foreign entity. Foreign entities by these concepts of data dispersion are when an entity had the control to manipulate data between the source and the client. It could be a foreign entity that manipulates the flow of data between two parties. These instances happen in our current decade and it seems that these attacks will not stop even after a few decades.

In computers and computer networks an attack is an attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyber attack is any

type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. Depending on the context, cyber attacks can be part of cyberwarfare or cyberterrorism. A cyber attack can be employed by nation-states, individuals, groups, society or organizations. A cyber attack may originate from an anonymous source.

A cyber attack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyber attacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities.

Cyberwarfare utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged cyber campaign or series of related campaigns. It denies an opponent's ability to do the same while employing technological instruments of war to attack an opponent's critical computer systems. Cyberterrorism, on the other hand, is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population". That means the end result of both cyberwarfare and cyberterrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace.

The flow of information is vast, and so is knowledge. Knowledge is power and as we seek on answers, some of us develop certain abilities that we can wield to take advantage of the others. One such example is the hackers of today's era. During the earlier periods of humanity, they are

the equivalent of snatchers and as we move on to the futuristic ideal of our society, such thieves will also exist. There are reasons why they exist. It could be because of financial problems. As any other or every individual's problems, the problem with money is common and cyber attacks and scams are now a usual problem of today's environment.

It is by the concept and relation of environment-problem crisis. Wherein it simply the relation of trouble makers in parallel to the community. Earlier times didn't have much security and so any complicated networks that we know of today so most of humanity relies and moves depending on physical movements. Thieves steal merchandises, tools, and money by grabbing and snatching with the awareness of its environment. Today, people or society are protected both by the physical and digital world. There are hidden cameras, CCTV's outside the streets to serve as evidence to physical problems. There's also the security on the internet. There are I.T. investigators. The ones who have the authority to catch people who do illegal activities via a network. This topic about security will be discussed more deeply on the following topics.

Those are the types of data deletion. There are stages that we consider life. In philosophy, you could say that there are no permanent things on this Universe. Everything will decompose and be transmitted or it will be a part of something new again. A new entity. Since we are talking about things, information is no different. This theory also proposes the idea that information is a thing.

Information is comprised of tiny bits. It could be a code, a series of smaller values that have representations that are being processed by a program which is also compromised of tiny bits or values. Just like we analyze every definition of an entity in this universe, every smaller case has its own representation and it will depend on the receiver whether it is complicated or basic. Like atoms on things, information is like the flow of energy, the power, and mechanism that lights up a smaller scale from a representation of zero. As some of us may know of, ones and zeros are

basic that is like defining whether something is on or off. Same things apply to information. The energy has its weight and the flow itself has an effect on the scale. It could be an effect on displacement, weight, and scale.

#### Elements of Information by Theory of Limited Information

Displacement - It is the changes on position of a particular particle or smaller division of energy or physical, the thermodynamic form that is being used into the formation of value in codes or any representational division for a larger value. To define the flow or the output whether it is on or off has value or no value.

Weight - the quality of an object that is a measure of the force by which the earth attracts it, or an object considered as having this quality of energy or a particle.

Scale - the size or level of something in comparison to what is average to the division of smaller value up to an understandable value.

#### Stages of Limitation by the Theory of Limited Information

##### The first stage of information limitation: Artificial Limitation

Artificial Limitation refers to the process of manipulating information as a stage by this theorem from the types of data dispersion wherein there are different ways on how the information is limited. It is commanded by the presence of a limit by a company. This stage refers to the start of contract from the client that can access information up-to-the set time; the start of contract from the client that can access information up-to the end where an interference occurred; the start of contract from the client that can access information up-to-the client wanted to end it.

##### The second stage of information limitation: Physical Bound Expiration

It is when information isn't considered as information with a series of ordered representing values and is according to the creator's goal. It also when a data is a loss due to its own expiration because of either of its own limited capacity or surrounding foundation. Surrounding foundation commonly refers to the hardware that stores data. If the hardware couldn't contain due to its ineligibility to do so because of many reasons and if the data is in an order that expresses an inaccuracy or in conflict to the creator's goals.

The third stage of information limitation: Time expiration

Time expiration is the data limitation wherein a data within a particular considered source cease to exist. It is when the elements that compromise the particular data didn't define the data as it is. It proposes that energy which composes the tiniest definable element of any data has a natural expiration which is the length of time. By the means of expiration, the energy wasn't able to be intact and starts to disperse which broke the foundation element of information. The element of scale as per definition of elements within the scopes of this theorem which only covered the scale as a measure to classify an information up to the smallest doesn't have anything to do with time as this element only serves as an element used into classifying the needed variables for any information. The weight which is comprised of energy itself, the mechanisms, the movement and any process related to the information is only parallel to the classified effects of any changes-outbound or inbound e.g. physical deterioration of mechanical, electrical parts, and energy transmission.

## References

Standardization), ISO (International Organization for. "Publicly Available Standards".

[standards.iso.org](http://standards.iso.org).

"ISTQB Standard glossary of terms used in Software Testing".

W., Lin, Tom C. (14 April 2016). "Financial Weapons of War". [ssrn.com](http://ssrn.com).

SATTER, RAPHAEL (28 March 2017). "What makes a cyberattack? Experts lobby to restrict the term". Retrieved 7 July 2017.

Lewis, James. United States. Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, D.C.: , 2002.

Web.